

January, 2015

Benefits, Payroll and Retirement Operations

Health Insurance Portability & Accountability Act (HIPAA)



Table of Contents

| | Page(s) |
|--------------------|---------|
| Definition | 1 |
| Overview | 2 - 3 |
| Health Information | 4 |
| Security & Privacy | 5 - 6 |
| Non-Compliance | 6 - 7 |
| Administration | 8 - 13 |
| Resources | 14 |

Definition

Health Insurance Portability & Accountability Act (HIPAA)

The Health Insurance Portability & Accountability Act, commonly known as HIPAA, was passed by Congress in 1996 to guarantee that individuals could move from one health plan to another without losing insurance coverage, or be denied coverage because of pre-existing conditions.

HIPAA addresses these major healthcare issues:

- Portability – the ability to transfer health insurance from one job to another
- Accountability – the prevention of health care fraud and abuse

HIPAA Privacy Rule

HIPAA's Privacy Rules are designed to address the public's concern for healthcare privacy. In addition to Protected Health Information (PHI), this includes Personal Identifier Information (PII) such as Social Security Numbers, birthdates, addresses and even zip codes. New technology increases privacy risk; e-mail, cell phones, Internet, etc.

- HIPAA creates national standards to protect PHI
- It also sets national boundaries on the use and release of health records
- Establishes appropriate safeguards for protection of PHI
- Strikes a balance to support disclosure for public health purpose
- Holds violators accountable – Civil and Criminal Penalties
- HIPAA gives people the right to an accounting of how their PHI has been disclosed and to obtain a list of individuals and agencies that have received their PHI
- Limits releases to the minimum PHI necessary
- Empowers people to control some uses and disclosures of their protected health information.

HIPAA also gives individuals the right to:

- Obtain a copy of a his/her medical records
- Request correction of medical records
- File HIPAA complaints with King County and/or Office of Civil Rights
- Have reasonable requests for confidential information communications accommodated
- Determine who can have access to their PHI. For example, an employee can authorize BPROS to discuss healthcare needs with a spouse or domestic partner and vice versa.

Overview

Who is Covered

HIPAA requirements apply to:

- Healthcare providers
- Health Plans – Government and Private
- Healthcare Clearinghouse: A private or public entity that facilitates the transfer of health information from a non-standard format into a standard format or receives standard information and processes it into a non-standard format
- Business Associates Relationships: Entities that conduct business on behalf of King County
- Business Associate Subcontractors: All of the downstream entities that receive, access, maintain and/or disclose PHI

King County is considered a hybrid entity because it is both a **provider** and a **plan** by having departments that provide:

- Health & Mental Health care
- Administration of the King County healthcare plan
- Reimbursement or payments for health care services received

Below is the **HIPAA Notice of Privacy Practice**. The full document can be found in the Regular Employee New Hire Guide, pages 30-31. For further information, go to: <http://www.kingcounty.gov/healthservices/MHSA/HIPAA/HIPAAlinks.aspx>

HIPAA Notice of Privacy Practices

Effective April 14, 2003



This notice describes how medical information about you may be used and disclosed by King County and how you can get access to this information.

Please review both pages of this notice carefully. If you have any questions, contact Benefits and Retirement Operations at 206-684-1556 or kc.benefits@metrokc.gov. For a copy of this notice, go to www.metrokc.gov/employees/benefits.

Our Obligations

We treat all personal information you provide us to administer your health benefits as confidential and, under the Health Insurance Portability and Accountability Act (HIPAA), we must:

- Maintain the privacy of any protected health information (personally identifiable medical information) you provide us when you enroll for benefit coverage, change coverage or ask for our assistance with a health benefit claim, except as indicated below.
- Provide you with this notice advising you how we handle your protected health information and informing you of our legal obligations and your rights regarding the information.
- Follow the terms of this notice effective April 14, 2003.

How We May Use and Disclose Protected Health Information

When you enroll for benefit coverage, change coverage or ask for our assistance with a health benefit claim, you provide us with confidential information such as your name and Social Security number. Sometimes, when you ask for our assistance with a claim, you may also provide us with details about the health treatments you've received and payments for services you've made. This information becomes protected health information when used and disclosed in the transactions required to manage our health care operations (administer your health benefits) and facilitate payment of health claims.

Pursuant to this notice, we may use and disclose this protected health information to:

- Our employees authorized to assist in the administration of county benefit plans
 - Representatives of the plans or any third party administrators with whom we have agreements to provide your benefit services.
- Additionally, we may use or disclose protected health information as follows:
- To the extent required by law
 - For purposes of worker's compensation or similar programs
 - When necessary to prevent a serious threat to the health and safety of you or the public or to respond to a disaster
 - To report suspected abuse or neglect as required by law
 - For law enforcement purposes as required or allowed by law
 - For specialized governmental functions including to correctional institutions if you are in jail or prison, as necessary for your health and the health and safety of others
 - To researchers, provided measures are taken to protect your privacy

Call 206-684-1556 for alternate formats.

- To business associates who provide services to us and assure us that they will protect the information from any unauthorized use or disclosure
- To a coroner, medical examiner or funeral director consistent with applicable state law as necessary to carry out their duties with respect to the decedent
- For public health and safety purposes as allowed or required by law including to public health authorities charged with preventing or controlling disease
- In the course of judicial/administrative proceedings in response to a court order or other lawful process
- To an oversight agency that is conducting an investigation of us as authorized by law.

For all the reasons explained above, we may use and disclose your personal health information without your written authorization. In all other cases, your written authorization is required.

Your Rights

For any protected health information provided to and maintained by us, you have the right to:

- Inspect and copy it
- Request amendments to it if it's incorrect or incomplete (we may deny amendment requests for specific reasons; for example, we deny requests to amend information we didn't create)
- Request to know to whom it's been disclosed for disclosures made after April 14, 2003 (the effective date of this notice)
- Request restrictions on what is disclosed and to whom (we try to honor restriction requests, but are not required to do so)
- Request it be communicated to you in a certain way (for instance, that we only contact you by mail or at work; we try to honor these requests, but are not required to do so)

You also have the right to cancel prior authorizations to use or disclose protected health information by providing us with written notice. Finally, you also have the right to receive a paper copy of this notice upon request.

To exercise any of these rights, contact us in writing. Mail your request to Benefits and Retirement Operations, Exchange Building EXC-ES-0300, 821 Second Ave., Seattle WA 98104-1566, or e-mail it to kc.benefits@metrokc.gov.

Changes to Our Privacy Practices

We reserve the right to change our privacy practices and to apply the new practices to protected health information we already have, as well as any information we receive in the future. We will notify you if we make changes and when the changes become effective.

Complaints

If you believe your privacy rights have been violated, you may file a complaint in writing with Benefits and Retirement Operations or the Secretary of the U.S. Department of Health and Human Services. You won't be penalized for filing a complaint.

To file a complaint with Benefits and Retirement Operations, mail it to Exchange Building EXC-ES-0300, 821 Second Ave., Seattle WA 98104-1566, or e-mail it to kc.benefits@metrokc.gov.

Health Information

Health information is any information, whether verbal, recorded or electronic, in any form that:

- Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearing house; and/or
- Relates to the past, present or future physical or mental health or condition of a individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual including demographic information.

Highly Sensitive Health Information

Highly Sensitive Health Information is considered any health information relating to:

- Testing for the Human Immunodeficiency Virus (HIV) or other sexually transmitted diseases.
- Treatment related to HIV or other sexually transmitted disease.
- Testing for cancer or other life-threatening illnesses.
- The diagnosis, treatment, or referral for treatment of a mental illness and/or alcohol or substance abuse.

Protected Health Information

Protected Health Information, or PHI, includes any health information, physical or mental health or condition of an individual, and any payment information for the provision of health care (includes demographic information) which either **specifically identifies the individual** it describes or **could be used to identify the individual**.

Within the scope of BPROS, PHI is any information obtained in the process of assisting employees with:

- Claims resolution
- Claims processing
- Claims payment
- Benefits enrollment information
- Processing payroll
- Processing W4 – W2 information

Security and Privacy

Maintaining Protected Health Information

In order to maintain the security of protected health information, BPROS has developed administrative policies and procedures that comply with HIPAA.

For Example: PHI is logged into the secure EBMS Case Log by authorized BPROS staff only and paper copies are filed in locked file cabinets and maintained in a secure location accessible only to BPROS staff.

In addition, the Human Resources Division has developed disaster recovery plans and business continuation plans for the EBMS Case Log.

PHI Security

Providing quality customer service includes protecting employee's confidential healthcare information. First, because it is required by law, and second because it helps employee's trust administrative offices within the county.

HIPAA:

- Is required by Law
- Earns employee trust
- Assures privacy of information
- Provides security of information
- Sets federal minimum standards and safeguards to protect PHI
- Preempts weaker state laws

As a King County employee, BA or subcontractor, you must be familiar with HIPAA policies and procedures so that you can show sensitivity and respect toward employees protected health and personal identifier information. You must respect each employee's right to privacy; treat all records as if they were your very own and be sensitive to privacy in all situations.

Inadvertent disclosures include all King County employees who may discuss or release PHI in the following situations:

- Grocery stores, car pools, van pools or family time
- Discussion or answering questions in public areas such as hallways
- Jammed fax or copier machines left unattended
- Leaving sensitive information unattended on desks
- Revealing more than minimum information necessary in ANY situation.

Security & Privacy

PHI Access

King County staff may have access to protected health information whenever:

- An employee or vendor provides information to receive reimbursement or to get help with a claim.
- Employees send an “Explanation of Benefits” form to BPROS to get help with a claim.
- PHI is communicated between King County and a Third Party Administrator or a benefit vendor such as Group Health, Washington Dental Service and Vision Service Plan.
- Processing payroll.
- Communicating payroll transactions with external agencies. (leins, garnishments, etc.)

In cases of non-compliance, progressive discipline is based on the personnel system:

- Civil Service personnel may face sanctions up to and including termination from service
- Commissioned Officers may face sanctions to include recommendation for termination of commission.

In addition to the penalties that Civil Service and Commissioned Officers may face for violating HIPAA rules, all King County employees may be held ***individually accountable*** under the Privacy act.

Given the serious nature of PHI privacy, even ***inadvertent*** disclosure is considered a serious infraction. Deliberate ***or*** inadvertent disclosure of PHI for any reason may lead to discipline up to and including termination.

The Privacy Officer takes every precaution to train employees on HIPAA Privacy Rules and how to properly secure PHI.

Non-Compliance

Civil Penalties

Fines for **civil** infractions are enforced by the Office of Civil rights as follows:

Civil Monetary Penalties:

- \$100 Per Violation
- Capped at \$25,000 for each calendar year for each requirement of prohibition that is violated.

Criminal Penalties

The **criminal penalties** for HIPAA violations includes greater penalties for knowingly violating the rules. Also, HIPAA violations can be severe enough to be considered a **criminal** offense and carry the following fines and jail time:

- Up to \$50,000 Fine & 1 year imprisonment for knowingly obtaining or disclosing individually identifiable health information.
- Up to \$100,000 & 5 years imprisonment if done under false pretenses.
- Up to \$250,000 & 10 years imprisonment if done with intent to sell, transfer or use for commercial advantage, personal gain or malicious harm.
- Criminal penalties are enforced by U.S. Department of Justice.

Privacy Officer

Each King County department has a designated **Privacy Officer** or contact person who is responsible for developing policies and procedures for HIPAA compliance. The Privacy Officer also handles disclosure complaints and resolves HIPAA issues.

- **Caroline Whalen** is the Privacy Officer for DES, which includes the LEOFF Disability Board.
- Public Health, DCHS and the Sheriff's Office each have identified privacy officers.

Administration

Training

King County provides HIPAA training to all employees. New employees receive training no later than 30 days after beginning work. Training must also be provided when policies and procedures are revised. BA & Subcontractor training is provided as needed.

Staff training is documented and maintained in writing or electronically for six years.

King County has policies and procedures to safeguard PHI for both electronic and paper records. These safeguards include administrative, technical and physical safeguards:

Administrative Safeguards includes orientation and termination policies, incident reporting policies, access, contingency and disaster recovery.

Technical Safeguards: User access and restrictions, user monitoring, authentication and password issuance.

Physical Safeguards: Physical access control during and after hours, shredding policies and health record removal from facility.

In addition, BPROS has taken steps to avoid inadvertent disclosures and minimize violations including:

- Identifying gaps in securing data
- Training, training and more training
- Monitoring HIPAA case law

When the county becomes aware of a HIPAA violation or PHI disclosure, reasonable steps are taken to ensure minimizing of the disclosure or violation. Any inadvertent disclosure must be documented, maintained and filed, along with a brief explanation of the resolution of the complaint.

Individuals that disclose HIPAA violations are granted the same protections and rights as any other disclosures covered under the Whistleblower Protection Code of King County.

The county does not tolerate retaliations or intimidating actions against an individual that discloses HIPAA violations or for participating in any process established for:

- Filing complaints
- Testifying
- Assisting or participating in an investigation, compliance review, proceeding or hearing.

Also, the county cannot force individuals to waive their rights to file complaints under the HIPAA Privacy Rule.

Administration

Disclosure Tracking Form


When any PHI disclosure occurs, it must be reported **regardless** of if the disclosure was intentional or inadvertent.

Each BPROS team member is required to keep a **Disclosure Tracking Log**. This log is used to record any incidence of PHI disclosure that they have done, witnessed, or in any way been involved. The log is sent as needed or quarterly to the Privacy Officer who reviews the log and takes appropriate actions.

Below is a sample **Disclosure Tracking Log**. You need to complete this information any time you are party to or witness an inadvertent or intentional disclosure of PHI. This log is a companion piece to the **Disclosure Form** (next page). These forms are turned in to the Privacy Officer (Cindy Lee) on an as-needed basis or quarterly.

May 2007

King County
Protected Health Information
Disclosure Tracking Log


King County

This log excludes authorized disclosures for treatment, payment and healthcare operations.

1. Disclosure Date: _____

Released To:
First Name: _____ Last Name: _____

Mailing Address: _____

City: _____ State: _____ Zip Code: _____

Phone (include area code): _____

Protected Health Information released: _____

Reason for releasing information: _____

Released By:
First Name: _____ Last Name: _____

2. Disclosure Date: _____

Released To:
First Name: _____ Last Name: _____

Mailing Address: _____

City: _____ State: _____ Zip Code: _____

Phone (include area code): _____

PHI released: _____

Reason for releasing information: _____

Released By:
First Name: _____ Last Name: _____

_____ Last Name: _____

_____ Zip Code: _____

_____ Last Name: _____

_____ Last Name: _____

_____ Zip Code: _____

_____ Last Name: _____

Completed Tracking Log to:
Privacy Officer, Cindy Lee
1 Second Avenue #300
MS: EXC-ES-0300
Seattle, WA 98104

Questions?
Contact Benefits and Retirement Operations by phone at 206-684-1556
or by e-mail at: kc.benefits@metrokc.gov

Administration

Disclosure Form

This is a sample of the **Protected Health Information Disclosure Form**. This is the form you would complete to report an *inadvertent* disclosure of protected health information.

May 2007

King County
Protected Health Information Disclosure Form

Please complete this form in response to an *inadvertent* protected health information (PHI) disclosure.

PART A
Name of person who disclosed PHI: _____
Job Title: _____ Department: _____
Phone: _____ Disclosure Date: _____
Describe *how* the PHI was inadvertently disclosed: _____

PART B
Please provide the following information for the person(s) whose PHI was disclosed:
First Name: _____ Last Name: _____
Mailing Address: _____
City: _____ State: _____ Zip Code: _____
Phone (include area code): _____

PART C
Please provide the following information on the person(s) who inadvertently received the protected health information:
First Name: _____ Last Name: _____
Mailing Address: _____
City: _____ State: _____ Zip Code: _____
Phone (include area code): _____

Continued...

Following information was released: _____
Appended to the information? _____
Information retrieved or destroyed? _____
Were taken to ensure a similar incident does not occur? _____
Person completing form: _____
Person completing form: _____
Privacy Officer (date): _____

Send completed form to:
DES Privacy Officer, Cindy Lee
821 Second Avenue #300
Mailstop: EXC-ES-0300
Seattle, WA 98104

Questions?
Benefits and Retirement Operations by phone at 206-684-1556
or by e-mail at: kc.benefits@metrokc.gov

Confidentiality Agreement

All BPROS staff (and certain other King County staff) must sign an annual **Confidentiality Agreement**. The agreement outlines the basic HIPAA rules and acknowledges that, as a county employee, you may have access to PHI. By signing the form, you are agreeing that you understand HIPAA and will abide by the policies, procedures and rules put in place by King County to secure protected health information.

May 2007

King County
Employee Access & Confidentiality Agreement

Security and confidentiality is a matter of concern for all persons who have access to King County benefits records and other confidential protected health information (PHI). Each person accessing this data and resources holds a position of trust and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. Therefore, all persons who are authorized to access King County benefits data and/or other PHI, and are physically located in the Benefits and Retirement Operations work area must read and comply with this Agreement.

As a King County employee you may have access either directly or indirectly to what this Agreement refers to as PHI. The purpose of this agreement is to help you understand your duty regarding PHI. Confidential information includes data related to employment records, disciplinary actions, medical information, beneficiary information, private health information and information proprietary to other companies or persons. You may learn of or have access to some or all of this confidential information in performing the duties assigned to the Benefits and Retirement Operations Section.

PHI and other confidential information is valuable and sensitive and is protected by law and by strict King County policies. The intent of these laws and policies is to assure that confidential information will remain confidential - that is, that it will be used only as necessary to accomplish the organization's mission. As an employee you are required to conduct yourself in strict conformance to applicable laws and King County policies governing confidential information. Your principal obligations in this area are explained below. You are **required to read and to abide by these duties**. The violation of any of these duties will subject you to discipline, which might include, but is not limited to, termination of employment and legal liability.

Accordingly, as a condition of and in consideration of your access either directly or indirectly to confidential information, by signing this document, you agree to:

- Respect the privacy and rules governing the use of any information accessible as a requirement in conducting your job.
- Not make unauthorized copies of records for your own use.
- Prevent unauthorized use of any information in files maintained, stored or processed by King County.
- Not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through your work assignment.
- Not exhibit or divulge the contents of any record or report except to fulfill a work assignment and in accordance with King County policy.

continued...

Benefits and Retirement Operations HIPAA Confidentiality Agreement

By signing this Agreement, I agree that I have read, understand and will comply with the Health Insurance Portability and Accountability Act King County Employee Access and Confidentiality Agreement.

Signature _____
Printed Name _____
Date _____

Return completed form to:
Benefits and Retirement Operations Section
821 Second Avenue #300
Mailstop: EXC-ES-0300
Seattle, WA 98104
Attn: Cindy Lee

QUESTIONS?
Contact BROS by phone at (206) 684-1556 or
e-mail: kc.benefits@metrokc.gov

Administration

Allowable disclosures of PHI:

There are some circumstances in which PHI can legally be disclosed. These include:

- When there is a request for treatment or payment of claims for healthcare procedures.
- When required by law or for public health purposes, to comply with worker's compensation and similar laws.
- When there is a request from an individual to review his/her PHI. However, a person may not look at the medical records of an adult dependent without written permission.

For example: A husband may not have access to his wife's medical records without her written consent, however; a parent could have access to a child's records if the child is **13 years old or under**.

May 2007

King County
Authorization to Disclose
Protected Health Information

I, _____, authorize the disclosure and/or use of my protected health information to:

(print full name)

Company/Organization: _____

First Name: _____ Last Name: _____

This authorization is valid from _____ to _____

(start date) (end date)

If no end date is indicated, this authorization expires twelve (12) months from date signed.

The type of information to be disclosed (check all that apply):

Enrollment: ☐ Eligibility: ☐ Claims: ☐ Other: _____

I understand that I have the right to revoke this authorization at any time and I must do so in writing and present my written revocation to the King County Benefits and Retirement Operations Section. Furthermore:

- This authorization to disclose my protected health information is voluntary.
- I understand that I can refuse to sign this authorization.
- I may inspect or copy the information to be used or disclosed.
- I understand that any disclosure carries with it the potential for unauthorized disclosure and the information may not be protected by federal confidentiality rules.

Printed name of person completing this form:

Signature of person completing this form:

Date: _____

Benefits and Retirement Operations Section
City/Lea Manager
821 Second Avenue #300
MS: EIC-ES-0000
Seattle, WA 98104
Phone: 206-464-1556
Email: kclb.hr@metrolink.gov

Authorization to Disclose_May 2007

BPROS must have a current signed **Disclosure Request Form** on file in order to disclose PHI about a spouse/domestic partner or dependent to the employee, or vice versa.

Administration

E-mailing Protected Health Information

In the course of day-to-day business, it may be necessary for BPROS staff to e-mail PHI. As much as possible, e-mails containing PHI must be sent using the county's Voltage encryption software.

However, there are times when sending encrypted e-mail is not an option. For example: several King County vendors are not able to open encrypted e-mails. In this case, all available and reasonable precautions must be taken to protect the information.

The following steps outline the process for sending PHI via e-mail when encryption is not an option:

1. Copy the PHI into a **Microsoft Word** document. If this is not possible, resave the document in its current program using the password protection guidelines in step two.
2. Save the Word document using the "**password protect**" feature.
3. The password formula is the month (written out completely, initial capped) that the document was created.
4. Send the password in a separate e-mail; never include the password with the protected information.

Although this method is not optimal, it does satisfy the HIPAA requirement by utilizing reasonable and available precautions in safeguarding PHI.

Administration

Alternatives

In addition to the rules, policies and procedures of protected health information, HIPAA grants individuals the right to request transmittal of PHI by **alternate means** or to an **alternate location**.

Alternate means are methods of sending confidential communications that are different from the usual methods. Usual methods are things like inter-office or U.S. mail. Alternate means would be e-mail, registered mail, hand-delivered, etc.

Alternate location means an address different from the mailing address. For example, the employee can ask to be contacted at work instead of at home or vice versa.

- The request must be submitted in writing and contain complete information about how the information will be sent, where the information is going and how it is to be addressed.
- The person making the request does not have to give a reason.
- The Benefits Manager or designee will approve or disapprove all requests. May only disapprove if request is not reasonable.
- Requests will be filed in the employee's benefits file after he/she has been notified of the decision of approval or disapproval.
- Above all, the request must be reasonable.

Resources

The following resources provide detailed information on HIPAA laws along with information on how King County abides by, and applies these laws. For specific questions about the county and HIPAA, contact the DES Privacy Officer, Caroline Whalen, via e-mail at: caroline.whalen@kingcounty.gov.

- **King County Benefits Web Site**
<http://www.kingcounty.gov/employees/benefits.aspx>
- **King County Benefits Payroll & Retirement Operations**
Phone: 206-684-1556
E-mail: kc.benefits@kingcounty.gov
- **Whistleblower Protection Policy**
<http://www.kingcounty.gov/operations/Ombudsman/whistleblower.aspx>
- **U.S. Department of Health & Human Services**
<http://www.hhs.gov/ocr/hipaa/>
- **U.S. Department of Justice**
<http://www.usdoj.gov/>